



Department of Homeland Security Daily Open Source Infrastructure Report for 25 April 2007

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Department of Homeland Security is warning U.S. chemical plants and bomb squads to guard against a new form of terrorism: chlorine truck bombs; the Chlorine Institute recently alerted the FBI to several thefts or attempted thefts of 150–pound chlorine tanks from water treatment plants in California. (See item [4](#))
- The Manhattan District Attorney's Office announced Friday, April 20, it has indicted 13 members of an identity theft ring that made more than \$3 million worth of illegal purchases using small hand–held devices to read and record personal information stored on the credit card's magnetic strip. (See item [9](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – <http://www.esisac.com>]

1. *April 24, World Nuclear News* — **Japan orders stricter checks at reactors.** The Japanese government will order special inspections of some nuclear power plants after recent revelations of past safety lapses. Trade minister Akira Amari said that the special inspections could force utilities to shut nuclear power reactors in advance of scheduled closures for mandatory inspections. Utilities were ordered by Amari to disclose past cases of safety lapses at their power plants by March 30. Ten nuclear utilities reported 316 cases of illegal operations at their

plants, including data falsification and safety breaches. Over all, 12 power utilities reported around 10,000 cases of falsification at nuclear, fossil and hydroelectric plants. The Nuclear and Industrial Safety Agency will put nine nuclear power reactors under stricter supervision and conduct extraordinary on-site inspections and checks. Inspectors will also be sent to 125 hydroelectric plants and five fossil power plants.

Source: http://www.world-nuclear-news.org/regulationSafety/200407-Japan_orders_stricter_checks_at_reactors.shtml

2. *April 23, Associated Press* — **Double-size fine for Indian Point.** The Nuclear Regulatory Commission fined the owners of the Indian Point nuclear power plant \$130,000 on Monday, April 23, for failing to meet last week's deadline for a new emergency siren plan. The commission said Entergy's action "significantly undermines the regulatory effectiveness of the NRC" and merited twice the usual \$65,000 fine for such a violation. Entergy said the sirens will be up "as soon as possible but not before it can be sure the new system meets the federal regulations, performs reliably and addresses the concerns of the emergency planning personnel from the four counties around Indian Point." The 150 sirens are meant to alert residents within 10 miles to any emergency at the plant. Despite extensive testing by Entergy, the sirens failed their final test on April 13. An existing 156-siren system with a spotty record is still operational and could be used if needed. On Monday, the commission gave Entergy 30 days to come up with an action plan specifying its strategy to get the new sirens up and working. Entergy said it would meet that demand.

Source: <http://www.chron.com disp/story.mpl/ap/fn/4740965.html>

3. *April 23, Department of Energy* — **DOE designates the Idaho National Laboratory Advanced Test Reactor as a National Scientific User Facility.** The Department of Energy (DOE) has designated the Idaho National Laboratory's (INL) Advanced Test Reactor (ATR) as a National Scientific User Facility. Establishing the ATR as a National Scientific User Facility will help assert U.S. leadership in nuclear science and technology, and will attract new users — universities, laboratories and industry — to conduct research at the ATR. This facility will support basic and applied nuclear research and development (R&D), furthering President Bush's Advanced Energy Initiative, which will advance the nation's energy security needs. Designation of the ATR as a National Scientific User Facility can directly contribute to the development of improved products and processes, encourages innovative scientific research, and will increase U.S. scientific competitiveness.

President's Advanced Energy Initiative:

<http://www.whitehouse.gov/news/releases/2006/01/20060131-6.html>

Source: <http://www.energy.gov/news/4987.htm>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

4. *April 24, USA TODAY* — **Chlorine bombs pose new terror risk.** The Department of Homeland Security (DHS) is warning U.S. chemical plants and bomb squads to guard against a new form of terrorism: chlorine truck bombs. At least five chlorine truck bombs have exploded in Iraq in recent months, killing scores of people and injuring many more after they breathed the toxic fumes. The Chlorine Institute, a trade group that represents more than 200 companies

that make and distribute chlorine, recently alerted the FBI to several thefts or attempted thefts of 150-pound chlorine tanks from water treatment plants in California. "This is now being used as a tactic against us in another part of the world," says Robert Stephan, DHS' infrastructure protection chief. "We've got to be prepared for it." The 150-pound chlorine tanks typically used in the bombs are "ubiquitous across the world," Stephan says. DHS officials are working with intelligence and Department of Defense officials to try to prevent similar acts in the U.S., he says. New federal regulations on chemical plant security are set to take effect this summer. DHS teams will begin inspecting hundreds of chemical plants that make and store chlorine and other potentially deadly chemicals.

Chemical Facility Anti-Terrorism Standards Interim Final Rule:

http://www.dhs.gov/xprevprot/laws/gc_1166796969417.shtm

Chlorine Institute: <http://www.chlorineinstitute.org/>

Source: http://www.usatoday.com/news/washington/2007-04-23-chlorine-truck-bomb_N.htm

5. *April 24, ABC 7 Chicago* — **Residents return to Illinois towns after evacuation.** Residents in three northern Illinois towns were allowed to return to their homes Tuesday, April 24, after a toxic chemical leak forced them to evacuate. A mandatory evacuation was ordered for the town of Seward, which is about 16 miles west of Rockford, after an anhydrous ammonia leak at Seward Agricultural Supply Inc. Residents of two neighboring communities, Pecatonica and Winnebago, were under a voluntary evacuation. Workers were moving ammonia from a tank to a truck when one of the hoses burst. Emergency crews wasted no time evacuating the town after they learned that hundreds, possibly thousands, of gallons of ammonia had spilled. After the spill, a toxic white cloud covered much of the small town. About 100 residents had to be evacuated immediately because ammonia can be fatal if too much of it is inhaled. The roads going into town were blocked off all night while the fire department and sheriff's deputies went door to door making sure everyone was out. Many of the evacuated residents spent the night at a couple local high schools. No residents or emergency workers were seriously injured but the toxic ammonia killed some residents' livestock.

Source: <http://abclocal.go.com/wls/story?section=local&id=5238924>

[[Return to top](#)]

Defense Industrial Base Sector

6. *April 24, Aviation Week* — **CBO warns of weapons cost inflation.** If weapons costs grow in the near future as they have over the past 30 years, spending requirements for the Department of Defense's (DoD) planned purchases in 2011 — excluding cost risk associated with ongoing wars in Iraq and Afghanistan — would average about \$195 billion annually, or \$19 billion more than the Bush administration has outlined, congressional budgeters have reported. But the non-partisan Congressional Budget Office (CBO), in an update released Monday, April 23, to its report on the long-term implications of current defense plans, projects that if weapons costs do not grow as they have historically, weapons research and development spending will continue to increase more gradually, reaching about \$195 billion by 2013 before falling off. Under those plans, the CBO said that during 2007–2011, Army investment would average \$29 billion, or 17 percent of total DoD investment. Navy and Marine Corps investment would average \$56 billion, or 33 percent; and Air Force investment would average \$60 billion, or 35

percent. Investment in other DoD activities would average \$26 billion, or 15 percent overall.

Source: <http://www.aviationweek.com/aw/generic/story.jsp?id=news/CBO042407.xml&headline=CBO%20Warns%20Of%20Weapons%20Cost%20Inflation&channel=defense>

[\[Return to top\]](#)

Banking and Finance Sector

7. *April 24, Reuters* — **ID theft task force urges tougher penalties.** A U.S. task force created to curb identity theft urged federal agencies on Monday, April 23, to help protect consumers by ceasing unnecessary use of Social Security numbers. A plan put forward by the Justice Department and Federal Trade Commission also recommended that Congress toughen and expand existing laws to make some identity thieves face a mandatory two-year sentence. The new plan called for measures requiring the private sector to safeguard personal data and notify consumers when a breach occurs and for creating a national identity theft law enforcement center for coordinating police investigations. Also it recommended legislative changes to help federal prosecutors charge those who use spyware, which can harvest personal data from a user's computer. The Center for Democracy and Technology said the government's new identity theft plan was a good start but that broader protections are needed for protection of consumer data and personal information.

Report: <http://www.ftc.gov/opa/2007/04/idtheft.shtm>

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/24/AR2007042400556.html>

8. *April 24, Reuters* — **China says U.S. piracy case will harm trade ties.** U.S. complaints to the World Trade Organization (WTO) over commercial piracy in China will "badly damage" cooperation, Vice Premier Wu Yi warned on Tuesday, April 24, insisting that China has made great strides in protecting patents and copyrights. Earlier this month, Washington launched two cases at the World Trade Organization claiming that Beijing was not doing enough to punish illegal copiers of films and music and that its restrictions on entertainment imports violated trade rules. China denounced Washington's move and Wu, who heads the country's economic dialogue with Washington, bluntly warned that the complaints would bruise bilateral trade ties. "The United States Trade Representative, the USTR, has totally ignored the massive strides China has made," Wu told an intellectual property forum in Beijing. Widespread bootlegging of films, music and software in China has long irked Washington, where many officials and lawmakers blame piracy for a portion of the massive U.S. trade deficit.

Source: http://www.nytimes.com/reuters/business/business-china-piracy.html?_r=1&oref=slogin

9. *April 22, ABC News* — **ID thieves use scanners to 'skim' credit cards.** Identity thieves have a new tool to steal credit card information — pocket-sized scanners that allow anyone handling your card to quickly record the personal information stored on it. The Manhattan District Attorney's Office announced Friday, April 20, it has indicted 13 members of an identity theft ring that made more than \$3 million worth of illegal purchases. Prosecutors say wait staff in Asian restaurants in Manhattan and along the East Coast were recruited to work as "restaurant skimmers." The skimmers allegedly used small hand-held devices to read and record personal

information stored on the card's magnetic strip. The stolen information was then used to make fake cards. There's no way of knowing if a credit card has been skimmed until fraudulent charges are made. The only sure way to protect yourself is to keep your card in sight at all times.

Source: <http://abcnews.go.com/WNT/LegalCenter/story?id=3066304&CMP=O TC-RSSFeeds0312>

[[Return to top](#)]

Transportation and Border Security Sector

10. *April 24, Associated Press* — JetBlue beats expectations revised in aftermath of storms.

JetBlue Airways' said Tuesday, April 24, that first-quarter losses had narrowed, but the discount carrier lowered expectations for 2007. JetBlue lost \$22 million, or 12 cents per share in the quarter, compared with a loss of \$32 million, or 18 cents per share, in the first quarter of 2006. Forest Hills, N.Y.-based JetBlue was roundly criticized earlier this year when it was forced to cancel more than 1,000 flights, stranding travelers in Northeast airports during the Valentine's Day snowstorm. Trying to control the damage in the storm's aftermath, JetBlue drafted a "customer bill of rights," under which the company issued vouchers to certain customers who experienced delays.

Source: http://www.usatoday.com/travel/flights/2007-04-24-jetblue-results-q1_N.htm

11. *April 24, Boston Business Journal* — Massport, Menino unveil plans for airport traffic. The Massachusetts Port Authority (Massport) and the City of Boston announced Monday two initiatives to encourage the use of clean fuel vehicles to and from Boston Logan International Airport, and throughout the city. Massport unveiled a plan that encourages Logan passengers and Boston taxis to drive to the airport in hybrid, alternative-fuel and alternative-powered vehicles. Mayor Thomas M. Menino announced a new \$25,000 grant to encourage the purchase of CleanAir cabs in Boston. Massport said as part of the initiative it is offering a preferred parking program to customers driving hybrid and alternative-fuel vehicles at the airport's Central garage, Terminal B garage, Terminal E surface lot and economy parking, starting Tuesday, May 1.

Source: <http://phoenix.bizjournals.com/boston/stories/2007/04/23/daily9.html>

12. *April 24, Associated Press* — Military jets scrambled to escort California plane. Military jets were scrambled to escort a commercial cargo plane to San Bernardino International Airport after the Boeing 727 crew failed to communicate properly, authorities said Tuesday, April 24. The jetliner, with Associated Air Cargo painted on its side, was en route to San Bernardino from Duluth, MN. It landed without incident Monday evening. "For whatever reason, it did not maintain adequate communication, and we alerted military escort," said Norm Brewer, spokesperson for the federal Transportation Security Administration. Brewer didn't know if it was a technical problem or a failure to follow protocol. "It was really a non-incident," Federal Aviation Administration spokesperson Mike Fergus said Tuesday. "It lost its communication ability and it was restored before landing." "It was determined there was no threat to security," Brewer said.

Source: http://cbs13.com/topstories/local_story_114153909.html

[\[Return to top\]](#)

Postal and Shipping Sector

13. *April 24, USPS News Release* — **New, easy international mailing.** The U.S. Postal Service's (USPS) most familiar and trusted mail products — Express Mail, Priority Mail and First-Class Mail — are going international starting May 14, 2007. To make it easier for customers to mail letters and packages worldwide, the Postal Service has simplified the eight main International Mail products into four: Global Express Guaranteed, Express Mail International, Priority Mail International, and First-Class Mail International. Another simplification for customers comes in packaging. Also effective May 14, mailers can use the same Priority Mail and Express Mail packaging whether they are shipping within the United States or to another country. And as always, the packaging supplies are available free of charge from USPS. Along with the product changes, USPS has restructured International Mail prices. In addition to the new International Mail options available for customers at post offices and online through usps.com, business customers may negotiate customized, flexible international shipping solutions based on the Postal Service's International Customized Mail agreements.

Source: http://www.usps.com/communications/newsroom/2007/pr07_033.htm

[\[Return to top\]](#)

Agriculture Sector

14. *April 23, Associated Press* — **Second Wisconsin herd has pseudorabies.** A second Clark County, WI, swine herd has contracted pseudorabies. The latest outbreak was found southeast of Loyal a week after a herd of 300 swine in the Greenwood area tested positive. The U.S. Department of Agriculture gave the state until May 2 to destroy the infected Greenwood herd and test all swine herds within five miles. A new quarantine zone has been established in the new zone around Loyal, which is slightly farther than five miles from Greenwood. The quarantine does not apply to other livestock. Experts say the disease, completely eradicated from commercial swine operations in the U.S. in 2003, could have been introduced to Clark County by feral pigs.

Pseudorabies information: <http://www.aphis.usda.gov/vs/nahps/pseudorabies/>

Source: <http://www.wbay.com/Global/story.asp?S=6415080>

15. *April 23, Michigan Department of Agriculture* — **Michigan issues quarantine to control spread of plant disease.** Michigan Department of Agriculture (MDA) Director Mitch Irwin Monday, April 23, announced the establishment of a state quarantine to prevent the spread of Plum Pox Virus (PPV). MDA detected the virus in a single plum tree east of Benton Harbor in fall 2006, resulting in portions of Berrien County being placed under federal restriction. The state's quarantine restricts movement of susceptible trees and plant parts near the location where the PPV was discovered, but does not affect movement of fruit from the area. PPV is a viral disease of stone fruit, such as peaches, nectarines, apricots, and plums and closely related ornamentals.

Source: <http://www.michigan.gov/mda/0,1607,7-125--166880--,00.html>

16. *April 23, Dallas Morning News* — Scientists perplexed by collapsing bee colonies.

Entomologists from across the country are meeting in Maryland on Tuesday, April 24, to puzzle over a strange phenomenon called Colony Collapse Disorder, where bees in 25 states so far leave their hives and never return. A German study blamed cell phones, but U.S. bee scientists say that theory is flaky. A Texas A&M bee biology professor blames bad corn syrup, but then why do some bees not fed this extract disappear as well? Pollination of U.S. crops and honey stocks worth \$14.6 billion is at risk. The syndrome is spreading to Canada and Europe. Tanya Pankiw, who teaches bee biology at Texas A&M University, finds the alarm about Colony Collapse Disorder overblown. "It's not like some huge epidemic," she said. "What we may be observing is not necessarily a disease or pathogen. There's some evidence to suggest a management practice" may be at fault. In 1997, Pankiw said, large numbers of bee colonies were lost because beekeepers fed them with a type of high-fructose corn syrup. "That may be what's happened here, but nothing's confirmed as a causal factor," she said.

Source: <http://www.ledger-enquirer.com/mld/ledgerenquirer/news/politics/17123671.htm>

[[Return to top](#)]

Food Sector

17. *April 24, Reuters* — U.S. to allow beef plant inspections by Japan. In a step aimed at expanding beef trade with Japan, the U.S. will allow Japanese inspections of U.S. beef plants, the Agriculture Department said Monday, April 23. Audits of processing plants will begin as soon as possible, Agriculture Secretary Mike Johanns said. "Once the verification process is complete, Japan will discontinue its requirement of inspecting 100 percent of the boxes of beef shipped from U.S. plants," he said. A Japanese agriculture ministry official said on Tuesday, April 24, that Japan wants to begin the inspections as soon as possible. Meat exporters have been working to rebuild their trade with Japan, which closed its market to U.S. beef at the end of 2003 when mad cow disease was discovered. Japan now accepts imports of U.S. beef from animals aged 20 months or younger, but U.S. exporters want to see meat allowed from cattle up to 30 months old. They also complain about the high costs of inspections for every box of imported meat.

Source: http://www.boston.com/news/world/asia/articles/2007/04/24/us_to_allow_beef_plant_inspections_by_japan_1177388814/

18. *April 23, Associated Press* — Ingredient imports underscore food supply vulnerability.

Billions of dollars worth of foreign ingredients that Americans eat in everything from salad dressing to ice cream get a pass from overwhelmed inspectors, despite a rising tide of imports from countries with spotty records, according to an Associated Press analysis of federal trade and food data. Ingredients are hard to quarantine and can go virtually everywhere in a range of brand products. When U.S. Food and Drug Administration inspectors at ports and border checkpoints look, they find shipments that are filthy or otherwise contaminated. They rarely bother to check in the first place, however, in part because ingredients aren't a priority. Because ingredients — oils, spices, flours, gums and the like — haven't been blamed for killing humans, safety checks before they reach the supermarket shelf are effectively the responsibility of U.S. buyers. Meanwhile, the ingredient trade is booming. Over the past five years, the AP found, U.S. food makers more than doubled their business with low-cost countries such as

Mexico, China and India. Those nations also have the most shipments fail the limited number of checks the FDA makes.

Source: <http://www.cnn.com/2007/HEALTH/04/23/imported.ingredients.ap/index.html>

19. *April 23, Washington Post* — **FDA was aware of dangers to food.** The U.S. Food and Drug Administration (FDA) has known for years about contamination problems at a Georgia peanut butter plant and on California spinach farms that led to disease outbreaks that killed three people, sickened hundreds, and forced one of the biggest product recalls in U.S. history, documents and interviews show. Overwhelmed by huge growth in the number of food processors and imports, however, the agency took only limited steps to address the problems and relied on producers to police themselves, according to agency documents. The outbreaks point to a need to change the way the agency does business, said Robert Brackett, director of the FDA's food-safety arm, which is responsible for safeguarding 80 percent of the nation's food supply. "We have 60,000 to 80,000 facilities that we're responsible for in any given year," Brackett said. Explosive growth in the number of processors and the amount of imported foods means that manufacturers "have to build safety into their products rather than us chasing after them," Brackett said. "We have to get out of the 1950s paradigm."

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/22/AR2007042201551.html?hpid=topnews>

20. *April 22, Central Valley Business Times (CA)* — **Tainted hog meat traced.** Hogs tainted with the chemical melamine at a Ceres swine operation have been traced from the farm to four other Northern California meat vendors, the California Department of Food and Agriculture (CDFA) said Sunday, April 22. The U.S. Food Safety Inspection Service says it was able to secure all product from American Hog Farm in Ceres that went to a federally inspected facility before it entered the commercial food supply, the CDFA says. Three other vendors are state-inspected facilities. Of those, one received animals during the time period in question that were not exposed to melamine-contaminated feed. At the property of another vendor, CDFA was able to account for and quarantine all of the exposed animals on-site before they could be sold. The third vendor, Bar None of Half Moon Bay, received hogs that were possibly exposed to contaminated feed. The CDFA says 42 pigs were purchased this month from the hog farm and may have consumed the feed.

Source: <http://www.centralvalleybusinesstimes.com/stories/001/?ID=4941>

[\[Return to top\]](#)

Water Sector

21. *April 23, CBS4 (FL)* — **New water rule announced to protect Everglades.** A groundbreaking rule was announced on Monday, April 23, that will guarantee water to protect and restore the Everglades. Following its passage last month by the South Florida Water Management District, the Regional Water Availability Rule went into effect. The rule prevents water users from tapping the famed River of Grass for new or additional supplies of water, which will set aside the water in the Everglades for environmental restoration. Permitted users like urban water utilities along Florida's southeast coast will now have to find alternative sources to supply regional growth. In South Florida, water suppliers in Miami-Dade, Broward, Palm Beach and Monroe counties currently depend on an estimated 500 million gallons of water per day from

the Everglades to recharge and sustain the Biscayne Aquifer, which is their primary drinking water source.

Source: http://cbs4.com/topstories/local_story_113143246.html

[[Return to top](#)]

Public Health Sector

22. *April 23, JHU Gazette* — **Malaria–infected mice cured by one dose of drug.** Johns Hopkins University researchers have cured malaria–infected mice with single shots of a new series of potent long–lasting synthetic drugs modeled on an ancient Chinese herbal folk remedy. The team also has developed several other compounds that defeated the febrile disease in rodents after three oral doses. These peroxide compounds, containing a crucial oxygen–oxygen unit, promise not only to be more effective than today's best malaria remedies but also potentially safer and more efficient, said research team leader Gary Posner. Though they say their results are very promising, the researchers caution that the new compounds must be thoroughly tested for safety and for how they are absorbed, distributed and metabolized in, and eliminated from, rodents' bodies before human tests begin.

Source: <http://www.jhu.edu/~gazette/2007/23apr07/23malar.html>

23. *April 23, NBC News* — **New Orleans health care under serious strain.** In New Orleans, LA, you can wait up to eight hours to see a doctor, and up to two days for a hospital bed. In the aftermath of Katrina, the New Orleans metro area has five fewer hospitals, and more than 2,600 fewer staffed hospital beds. There is a critical shortage of nurses. To replace them, hospitals are going to extremes. "The only place we found any quantity is in the Philippines and India," says Jack Finn of the Metropolitan Hospital Council of New Orleans. "We are bringing them in from out of the country." Before Katrina, the uninsured would have gone to Charity, the city's only state–funded hospital. But today, Charity remains in ruins. With no place else to go, the uninsured head for the city's remaining emergency rooms, adding to the lines and draining away money that could have paid for more space, more beds and more staff.

Source: <http://www.msnbc.msn.com/id/18274893/>

[[Return to top](#)]

Government Sector

24. *April 24, Government Accountability Office* — **GAO–07–724T: Federal Transit Benefits Program: Ineffective Controls Result in Fraud and Abuse by Federal Workers (Testimony).** Under the federal transit benefits program, federal employees receive transit benefits (e.g., Metrocheks) to encourage them to commute to work via public transportation. Based on information provided by the Department of Transportation, as of July 2006, the National Capital Region had 120,000 participants claiming roughly \$140 million in benefits. Recently, inspectors general (IG) of various agencies have found numerous prior instances of fraud, waste, and abuse in this federal program. Based on both the significance of these IG findings and the amount of federal money spent on transit benefits, the Government Accountability Office (GAO) was asked to (1) investigate allegations that federal employees in

the National Capital Region are involved in fraud and abuse related to the transit benefits program, (2) identify the potential causes of any fraud or abuse that is detected, and (3) estimate the magnitude of fraud and abuse in the National Capital Region in 2006. To address these objectives, GAO identified federal employees selling their transit benefits on the Internet and obtained additional data from these sellers' employing agencies to determine whether more widespread problems existed. GAO also obtained the policies and procedures governing the transit benefits program at each of the employing agencies.

Highlights: <http://www.gao.gov/highlights/d07724thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-724T>

25. *April 24, Government Accountability Office* — **GAO-07-755T: Capitol Visitor Center: Update on Status of Project's Schedule and Cost as of April 17, 2007 (Testimony).** Since the March 13, 2007, Capitol Visitor Center (CVC) hearing, the CVC team has continued to move the project's construction forward, but the Architect of the Capitol (AOC) has extended the project's scheduled completion date by about two months, to June 2008, and further delays are possible. This delay was attributable to problems with activities on the project's critical path — the fire protection system. AOC will be able to meet or come close to meeting its new scheduled project completion date only if the CVC team promptly makes significant improvements in its execution of the project and the project's schedule. To date, AOC's implementation of actions identified in its November 2006 action plan has not been completely effective in curtailing additional schedule slippages. As the Government Accountability Office (GAO) reported at the last CVC hearing, GAO previously estimated that the total cost of the entire CVC project at completion would likely be about \$592 million without an allowance for risks and uncertainties, and over \$600 million with such an allowance. Because of the uncertainty over the project's expected completion date, GAO has not updated these estimates. Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-755T>

26. *April 22, Daily Times (MD)* — **Campus security takes center stage on Maryland's Eastern Shore.** The Virginia Tech tragedy has raised awareness among students and faculty members on the importance of communication in an emergency situation. Some VT students complained they received no warning with the exception of an e-mail that arrived more than two hours after the first shots were fired. In addition, both cellular voice and e-mail services were overloaded in minutes following the incident. However, text messages — requiring much less bandwidth — got through consistently. University of Maryland Eastern Shore's (UMES) HawkTalk program includes a wireless "Broadcast Alert" feature that allows the school to send a text message to every registered user in one step. This feature enables critical emergency information to go to the university community immediately; in most cases, in less than a minute. "One of the things we really focused on was communication services with the students on campus," said Ron Forsythe, vice president for planning assessment, technology and commercialization at UMES. "If you call the residential hall, you can't get in touch with them." The most unique feature is the Rave Guardian, which allows university officials, upon a student's request, to track the student's route by integrating GPS tracking into the institution's public safety system. Source: <http://www.delmarvanow.com/apps/pbcs.dll/article?AID=/20070422/NEWS01/704220303/1002>

Emergency Services Sector

27. *April 20, San Jose Mercury News (CA)* — **Short quake warning could save lives.** After a devastating earthquake hit the Hayward Fault in 1868, a Bay Area physician shared what sounded like a half-baked idea at the time: Use wires and electric currents to sound alarm bells at the start of a major earthquake, giving a short warning to people living away from the epicenter. The idea is likely to become reality in California within the next decade, many seismologists now believe. Even though 10 to 20 seconds' warning might not sound like much, it could make quite a difference, experts say. It could allow Caltrain and Bay Area Rapid Transit officials to slow down trains and reduce the risk of derailments. Fire stations could open their garage doors and get their engines ready to roll. Interstate metering lights could all be turned to red to keep vehicles at a stop. Elevators could be programmed to open at the nearest floor to prevent people from getting trapped when the quake hits. Government and private university workers are now testing an early prototype for an earthquake warning system — one that works by measuring the fastest-moving waves from a quake, and sending an alert before the slower but more devastating waves hit.

Source: http://www.mercurynews.com/celebrities/ci_5710993

[[Return to top](#)]

Information Technology and Telecommunications Sector

28. *April 24, Information Week* — **Malware spikes in 1Q as hackers increasingly infect Websites.** The number of new pieces of malware spiked in the first quarter of this year, and the majority of the new threats are being embedded in malicious Websites. According to a study from Sophos, an antivirus and anti-spam company, researchers discovered 23,864 new threats in the first three months of 2007. That's more than double the number of new malware identified in the same period last year, when Sophos discovered 9,450. While the number of malware is increasing, where it's being found is changing. Historically, malware has plagued e-mail, hidden in malicious attachments. While that's still happening, more virus writers are putting their efforts into malicious Websites. Sophos noted that the percentage of infected e-mail has dropped from 1.3 percent, or one in 77 e-mails in the first three months of 2006, to one in 256, or just 0.4 percent in this year's first quarter. In the same time period, Sophos identified an average of 5,000 new infected Web pages every day. With computer users becoming more aware of how to protect against e-mail-based malware, hackers have turned to the Web as their preferred vector of attack.

Sophos study: <http://www.sophos.com/pressoffice/news/articles/2007/04/reportapr2007.html>

Source: <http://www.informationweek.com/news/showArticle.jhtml;jsessionid=2O4TQMKELEDQSNDLRCKH0CJUNN2JVN?articleID=199201032>

29. *April 23, ComputerWorld* — **Microsoft: No patch yet for DNS Server bug.** Microsoft Corp.'s security team Sunday, April 22, said it is still working on a patch for a critical bug in the company's server software. The vulnerability in the Domain Name System (DNS) Server Service of Windows 2000 Server SP4, Windows Server 2003 SP1 and Windows Server 2003 SP2, has been exploited since at least April 13, Microsoft acknowledged earlier — although the

company has continued to characterize those attacks as "limited." "Our teams are continuing to work on developing and testing updates...[but] we don't have any new estimates on release timelines," said Christopher Budd, program manager for the Microsoft Security Response Center (MSRC) on the group's blog. "I can say that our ongoing testing so far has not raised any issues that would make us believe we might be looking at a longer timeline." MSRC blog:

<http://blogs.technet.com/msrc/archive/2007/04/22/sunday-update-on-microsoft-security-advisory-935964.aspx>

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017540&intsrc=hm_list

30. *April 23, ComputerWorld* — **Safari, Firefox, IE all vulnerable if QuickTime is installed, say researchers.** The vulnerability that put \$10,000 into the pocket of a New Yorker last Friday, April 20, during a Mac hacking contest is in Apple Inc.'s QuickTime media player, researchers said Monday, April 23. The contest, held at the CanSecWest security conference in Vancouver last week, pitted a pair of MacBook Pro notebooks, each with all currently-available security patches installed, against all comers. On Friday, Sean Comeau, one of the CanSecWest organizers, said the bug was in Safari, the Apple browser bundled with Mac OS X. But Monday, researchers at Matasano Security LLC, a New York-based consultancy, said the flaw is actually in QuickTime. "Dino's finding targets Java handling in QuickTime," said Matasano researcher Thomas Ptacek on the group's blog. "Any Java-enabled browser is a viable attack vector, if QuickTime is installed. Apple's vulnerable code ships by default on Mac OS X (obviously) and is extremely popular on Windows, where this code introduces a third-party vulnerability." Ptacek confirmed that both Safari and Mozilla Corp.'s Firefox can be exploited through the new QuickTime bug. Matasano also said it assumes that Firefox is vulnerable on Windows PCs if QuickTime's plug-in is installed.

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017598&intsrc=hm_list

31. *April 16, Government Computer News* — **Solar flare puts GPS off the air.** Mysteriously, on December 6, 2006, Global Positioning System (GPS) devices suddenly malfunctioned across large swaths of the planet. The cause was an intense burst of radio energy, called a solar flare, emitting from the sun's surface. Although the event temporarily knocked out many GPS receivers, no airplanes fell from the sky, and no ships lost their way at sea. But the event nonetheless generated concern among scientists. Although they were aware that radio bursts generated by solar flares could affect GPS equipment, they were surprised that this large an event occurred during a period of relatively low solar-flare activity and that its impact was as strong as it was. "It's more serious than we thought. We didn't think this was going to happen until the next solar maximum, which is about 2011," said Paul Kintner Jr., professor of electrical and computer engineering at Cornell University. "We've been monitoring solar flares for four years. [The Dec. 6 event] suggests that monitoring has been inaccurate. And we don't have a good historical basis for predicting what's going to happen, so we're concerned." The radio bursts don't actually damage equipment but only interfere with transmissions between GPS satellites and receivers.

Source: http://www.gcn.com/print/26_08/43512-1.html

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.